

Smart Grids in the European data protection legal framework

Smart metering implications for the EU data protection



*University of Oslo
Faculty of Law*

Candidate: Daniela Havlíková

Supervisor: Tobias Mahler

Deadline for submission: December/1/2011

Number of words: 17,712 (max. 18.000)

25/11/11

Abstract

Smart Grids are electricity networks of tomorrow that offer many benefits to its users. As with any other technology, there are also problematic issues that need to be solved before the beginning of a widespread deployment of intelligent grids in the European Union.

Critics point out that data protection and privacy could be threatened by installment of smart metering technology. These intelligent meters enable collecting personal data from each household or company on an unprecedented scale as well as remotely connecting/disconnecting smart appliances from electricity. Whereas some people welcome the possibility to lower their energy consumption, others are afraid that the privacy of their homes will be threatened.

To what extent is the EU legislation able to respond to these concerns and protect people against some of the unintended impacts of Smart Grids needs to be evaluated. This thesis is considering those concerns, presents the current data protection legal framework and provides a legal analysis of the main provisions that might concern Smart Grids. Second part of the thesis is considering non legislative options for data protection in Smart Grids as well as it evaluates current EU efforts in this field.

Content

ABSTRACT.....	2
CONTENT.....	3
1. INTRODUCTION.....	5
1.1 LEGAL QUESTIONS AND PROBLEMS CONSIDERED (MAIN RESEARCH QUESTIONS).....	6
1.2 METHODOLOGICAL APPROACH	7
1.3 DEFINITIONS	8
1.4 TECHNICAL ASPECTS OF SMART GRIDS.....	9
2. THE LEGAL FRAMEWORK REGARDING PRIVACY, DATA PROTECTION AND SMART GRIDS/SMART METERING	13
2.1 LEGISLATION CONCERNING PRIVACY AND DATA PROTECTION.....	13
2.2 EU LEGISLATION REGARDING THE SMART GRIDS/SMART METERS.....	18
2.3 THE EUROPEAN UNION DOCUMENTS CONCERNING SMART GRIDS.....	21
3. LEGAL ANALYSIS.....	26
3.1 DATA PROCESSING.....	26
3.2 DISTINCTION BETWEEN DATA CONTROLLER AND DATA PROCESSOR.....	28
3.3 REQUIREMENTS FOR THE PROCESSING OF PERSONAL DATA	30
3.4 DATA SUBJECT CONSENT	32
3.5 CONTRACT.....	34
3.6 LEGAL OBLIGATION.....	35
3.7 LEGITIMATE INTERESTS.....	36

3.8 DATA RETENTION.....	37
3.9 THIRD PARTIES PROCESSING OF PERSONAL DATA (VALUE ADDED SERVICES).....	39
3.10 PRIVACY IN THE SMART METERING.....	41
4. RECOMMENDATIONS ON SMART GRIDS/SMART METERING AND DATA PROTECTION...	46
4.1 PRIVACY BY DESIGN (PRIVACY ADDRESSED AT THE DESIGN PHASE).....	47
4.2 ANALYSIS OF THE RECOMMENDATIONS OF THE EXPERT GROUP 2 (DRAFT JUNE 2011 REPORT).....	50
5. CONCLUSION.....	55
6. REFERENCES.....	57
7. ANNEXES.....	61

1. Introduction

The era of rapid information and communication technology (ICT) development brings new aspects to our lives. Also electricity, water or gas deliveries are becoming subject of this era. Networks that bring us these vital sources are ageing and showing their limits in the terms of responding to new environmental and societal challenges. One of the responses of governments and other interested stakeholders is trying to develop electrical grids of the future, such as by developing the concept of Smart Grids, smart meters and smart appliances. The use of new ICT technologies in the energy infrastructure could present a great opportunity in enhancing peoples lives in an energy efficient way. The European Commission is trying to support the development of Smart Grids across the EU by stressing their benefits in a number of official or unofficial documents.¹ Main advantages of Smart Grids can be summarized as follows: more efficient use of electricity, cheaper and safer operation of the grid, control and management of consumptions patterns for consumers, direct communication among energy actors (households, companies, consumers, energy suppliers and other grid users), greater ability of avoiding blackouts, and quicker restoration of the power when outages occur.² Smart Grids also allow for integrating more electricity produced from renewable energy sources and at the same time leave space open to the conventional power generation. They also make charging electric vehicles easier (as its/their use can also be for the excess power). Smart Grids bring however also issues that need to be handled with care. Critics across the world stress problems with privacy, data protection, cyber-security or health issues that need to be addressed. The European Commission is aware of these challenges, in the report of its Joint Research Centre states: "Either directly or indirectly, consumers will be affected by several threats (natural threats, smart thieves, hackers, terrorism, warfare,

¹European Commission, *Smart Grids: from innovation to deployment; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, Brussels, 12.4.2011

²The safety of Smart Grids can be questionable in the view of potential vulnerability to hacking and cyber attacks

accidental threats, intentional attacks, load shedding).”³ This shows that proper safeguards should be in place before mass implementation of Smart Grids. The European Commission is working on a number of recommendations in this respect (more will be presented in the chapter 4.2). It is necessary to critically assess these efforts. Therefore, focus of this thesis will be on evaluating how is the European data protection legal framework prepared to include Smart Grids, more specifically smart metering.

1.1 Legal questions and problems considered (main research questions)

I will consider legal questions regarding the applicability of the European data protection framework to Smart Grids/smart metering. Specifically, I will consider whether it is necessary to prepare specific legislation for Smart Grids. Evaluation whether the current legal framework is sufficient (satisfy the data protection and privacy criteria) - in a sense that it would enable including Smart Grids in the legal framework will be provided.

European data protection framework can vary among all EU members due to the different implementation of the Directives (eg. Directive 95/46/EC on the protection of the personal data - Data Protection Directive).⁴ Experts claim that with the specific situation of Smart Grids it is necessary to prepare *sui generis* legislation (for example to adopt an EU regulation – applicable to all EU states).⁵ I will consider whether this kind of regulation is necessary.

³Joint Research Centre, *Smart Grid projects in Europe: lessons learned and current developments*, 2011, available at <http://ses.jrc.ec.europa.eu/images/stories/deliverables/jrc%20report%20-%20smart%20grid%20projects%20in%20europe.pdf>, September 2011: Cyber security will not be mentioned in detail in this thesis

⁴ See Directive 95/46/EC (Data Protection Directive) Note: Full citations to all directives are available in the IReferences section *Infra*.

⁵ “There may be a need for a legislative proposal for a sector-specific directive on smart grid data protection to complement the [EU] data protection framework, namely the EU Data Protection Directive, the e-Privacy Directive and the Data Retention Directive.” in Utility Week (1. July 2011), http://www.utilityweek.co.uk/news/news_story.asp?id=195596&title=EU+smart+grids+privacy+legislation+under+discussion, accessed on 26.7.2011

In order to ensure the rights of individuals for privacy and data protection, the concept of Privacy by Design is suggested by experts (Ann Cavoukian, Expert Group 2).⁶ I will consider whether Privacy by design/default is the solution to the Smart Grid privacy and data protection issues. Also other technical solutions and legislative options will be evaluated.

This thesis will not deal with the security in Smart Grids, cyber-security issues, standards, regulators, telecommunications and measuring systems.

1.2 Methodological approach

The primarily focus of this thesis will be to answer the question whether the current European data protection framework regarding Smart Grids/smart metering is sufficient for their deployment. Therefore, I will first consider available EU legislation governing data protection, privacy and Smart Grids (focus will be on the EU level, not on national jurisdictions). For a better understanding of the Smart Grids functionalities, basic technical aspects will be presented. In the legal analysis, the applicability of the current data protection and privacy laws (*de lege lata*) would be discussed in detail and some improvement for possible new legal framework (*de lege ferenda*) suggested. Additional focus will be placed on privacy by design/default solutions that might enhance further legislation processes. Concluding remarks will critically discuss the proposed solutions made by the Task Force on Smart Grids (the second Smart Grid Expert Group) that came with a draft report in June 2011.⁷ The above mentioned report could become the future basis of a new legal framework for Smart Grids. Some of the suggested solutions are to prepare a new regulation or a maximum-harmonisation directive. This thesis will end its

⁶This is elaborated further in chapter 4

⁷Task Force Smart Grids, Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection- final draft*, issued on 6.6.2011 available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_draft.pdf, accessed on September 2011

research in November 2011 whereas the work of the European Commission continues further.⁸

Most of the current legal articles and documents discuss mainly the privacy and data protection implications of smart meters/intelligent metering, other components of Smart Grids are omitted. This thesis will also focus primarily on smart meters as a main point of legal analysis. Smart Grids will be left to a more general description.

1.3 Definitions

Currently, there is no standard global definition of Smart Grids and its functionalities. One can choose from numerous explanations such as that Smart Grid is more like an umbrella term covering IT solutions for transmission and distribution grid. For the purpose of this thesis, following definition will be used:

Smart Grid⁹ is “*upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added.*”¹⁰

Intelligent metering can be also defined differently (as in the above mentioned case of Smart Grids).¹¹

⁸According to the European Data Protection Supervisor, there was a meeting of the Expert Group 2 in November 2011, the outcomes of this meeting are not yet publicly available; also the review of the Data Protection Directive that was planned to this year seem to be postponed to 2012 – Latest information can be checked here:

http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm;
http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

⁹This thesis will be using capital letters for Smart Grids and small letters for smart meters in order to unify with the official EU sources such as (European Commission documents or Task Force Smart Grids, Expert Groups). This might differ from other materials and documents.

¹⁰European Commission, *Smart Grids: from innovation to deployment*

¹¹Among other definitions used by the EU organs is for example: “Smart Grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.” Task Force Smart Grids, Expert Group 2: Regulatory Recommendations for data safety, data handling and data protection, report issued 16.2.2011 (available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf), accessed on July 2011

Smart metering – “There is no standard definition¹² of smart metering, but it usually refers to using advanced meters in conjunction with communication systems to allow customers to monitor their energy consumption in real time.”¹³

1.4 Technical aspects of Smart Grids

In order to understand the complexity of legal issues that need to be covered, it is necessary to describe the technical part of Smart Grids. The traditional electricity system, “the dumb” system, that transports electricity generated by power plants is no longer capable to cope with challenges of modern electricity consumption.

To present some of the main problems: increasing energy demand requires more resources for energy production, the network is not capable to integrate all energy from renewable energy sources, there is a risk of instability of the network and possible power shortages if the grid is overloaded, need to shift from fossil fuels to sustainable energy sources. The “smart” part of the new grids consists of the ICT solution that uses digital technology to transmit, distribute and deliver power to end consumers. The old (dumb) system will become a two flow/bi-directional network that enables information exchange between supplier and user and better side-demand management. Development of the new grid requires a lot of work on technology, standards, policy and regulatory frameworks.

Important component of Smart Grids is **smart metering**.¹⁴ It is the last step among customers and energy delivery. Smart meters are typically equipped by a two-way communication functionality that records household energy consumption data and communicate them to the power distributor. Collection of such data is much wider than by the traditional meters that were read physically few times a year. The key abilities of the new meters lie in remote reading of the meter data in real time for the provider as well

¹²Among other definitions used by the EU is for example: “Smart metering is designed to provide utility customers with information about their domestic consumption.” Task Force Smart Grids, Expert Group 2: Regulatory Recommendations for data safety, data handling and data protection, report issued 16.2.2011 (available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf), accessed on July 2011

¹³Smart meters: Controlling your energy bill? (available at <http://www.euractiv.com/en/energy-efficiency/smart-meters-controlling-your-energy-bill-links-dossier-257199>), accessed on July 2011

¹⁴Smart meter usually measures electricity but can be also used for gas, water or heat meters

as the fact that consumers can monitor their own energy consumption (for example on a web portal). The problems that are connected to the use of smart meters will be in detail presented in the next chapters. Intelligent meters may also potentially communicate with a number of appliances within our homes. Some of the world's main manufacturers started to develop and sell the so called **smart appliances**. These smart refrigerators, washing or dishwasher machines would communicate with the smart meters and provide them with real time information of the electric use on the appliance level. If the consumption would be too high or too low, the utility might be able to switch these appliances on/off according to the preference of the customers.

To understand Smart Grids better, it is useful to present main actors in this field. There is a distinction among electricity networks – European Power Grid is connected with regional electricity grids by high-voltage grids. **Transmission system operators (TSOs)** manage the high voltage grid, 110 kilovolt (kV) or higher and monitor the reliability and continuity of the national electricity retail (they are responsible for correcting the imbalance in demand and supply).¹⁵ The energy distribution in medium and low voltage grids is the responsibility of the **Distribution system operators (DSOs)**.¹⁶ Among their important tasks are the overall power grid stability and operational security. The DSOs will also become main players in smart metering (in some countries, not all EU Member States). They will be responsible for the installation and running of the smart meter system as well as determination of how the data is stored, collected and used.¹⁷ The DSOs should also be involved in active network and load management as well as electricity storage.¹⁸ Expert Group 2, June 2011 report, describes in detail some of their tasks:

”DSOs will have detailed information on the status of the network components [...]”

¹⁵Expert Group 2, draft report from 6.6.2011

¹⁶Distribution system operator =Distribution service operator as it is described in the Art.29 Data Protection Working Party Opinion 183 on smart metering

¹⁷Art.29 WP Opinion 183 on smart metering, DSO's will be data controller in the above mentioned case – this will be elaborated further

¹⁸Active power grid network interacts with renewable energy sources and distributed generation; local load management is for avoiding network congestions (it can reduce impacts on higher voltage levels); electricity storage – DSOs can have storage facility which they offer to other energy players

energy flows.[...] This includes secure remote reading of resident customers' metrological registers.”¹⁹ Good cooperation between TSOs and DSOs will be important for the future Smart Grids, in areas such as exchange of information or forecast of the overall system load. The above mentioned operators are not the only ones dealing with Smart Grids, there are also **Energy Market Suppliers** who are responsible for energy supply to consumers, procurement of energy from their own sources (wholesale markets) and for billing and serving customers.²⁰ In some countries (e.g. UK), energy supplier takes over the tasks of DSOs. It is important to distinguish DSOs from Energy Market Suppliers since both can have different legal roles (according to their responsibilities in the Member States).²¹

The technical part of Smart Grids is complex and involves many more actors than those mentioned above. The ICT and telecommunication sectors will be additional key elements in Smart Grids deployment.²² As in the case of different ICT solutions (telecommunication sector or internet), the technology matures and is thus important to prepare technology neutral legislation which would reflect changes in time. One needs to bear in mind that this will be a lengthy process since the Smart Grids technology will be introduced gradually.

As the Expert Group 2 report from June 2011 states: “the course of Smart Grids adoption in Europe is far from clear, the underlying technologies remain expensive; their business case relies on assumptions of significant changes in customer behaviour; and cost-effective integration of existing systems and emerging technologies is not yet proven.”²³

Those issues should be of the main concern of the European Union authorities. It is

¹⁹Expert Group 2, draft report from 6.6.2011

²⁰Ibid.

²¹This will be shown in the chapter on data controller

²²Internet protocols (IP) will be used as a core technology of Smart Grid (EG 2 June 2011 report); IPv4 and the next generation IPv6 will contribute to the Smart Grids deployment in EU (much of the smart appliances need to be working with the IPv6 because of shortage of the current IPv4 addresses)

²³ Expert Group 2, draft report from 6.6.2011, page 79

necessary to assess all the risks and prepare regulatory framework which enables smooth implementation of Smart Grids in the Member States. To what extent is European legal framework prepared for Smart Grids/smart metering will be evaluated further.

2. The legal framework regarding privacy, data protection and Smart Grids/smart metering

2.1 Legislation concerning privacy and data protection

The European privacy and data protection lies on two main pillars: the European Convention on Human Rights (ECHR) and the EU legal instruments of which the most important are the Charter of the Fundamental Rights and Data Protection Directive. Even though there are also other international and European instruments, the above mentioned legal sources will be of most value to this work. In order to understand how privacy and data protection legislation can be applied to Smart Grids, it is useful to present the current legal framework that governs privacy and data protection policies in Europe.

2.1.1 International human rights law

The Council of Europe has passed legislation that became the basis for human rights in Europe (and in signatory countries), **the European Convention on Human Rights** (ECHR). Article 8 of the ECHR titled *Right to respect for private and family life* is one of the most important legal sources in this area. Essential objective of this article is to protect individuals against interference by public authorities in his/her private life.

“1. Everyone has the right to respect for his private and family life, his home and correspondence.

*2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.*²⁴

²⁴European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 (ECHR)

Since this Convention was drafted in the 1950s and entered into force on 3.9. 1953, some of its articles might seem outdated in the light of new technological developments. But the case law shows us that ECHR can be interpreted according to the economic and technological developments (for example correspondence can also be applied to email or other electronic communication). Some scholars and experts thus claim that Article 8 is also applicable to Smart Grids/smart meters. This right usually needs to go through a privacy test and satisfy the criteria of legality, necessity (proportionality) and legitimacy. Usually, the last criteria could be used in favour of Smart Grids roll-out. This will be shown later.

2.1.2. Current EU legal framework for data protection

The EU data protection law is the most developed (in the world) since data protection is now recognized as fundamental human right, independently of the right to privacy. When the Lisbon Treaty entered into force, **the EU Charter of Fundamental Rights (CFR)** became legally binding. It is important to mention the wording of Article 8 of the CFR since it includes a separate article on data protection.

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”²⁵

If we look at the Article 7 of the CFR, one can see that the wording is similar to the Article 8 ECHR with the exception of communications (that were not mentioned in the latter).

Article 7 “Respect for private and family life

²⁵ Charter of Fundamental Rights of the European Union (CFR), art. 8, 2000 O.J. (C 364) 1 (2000) (receiving full force of law after entry into the Lisbon treaty of 2009)

Everyone has the right to respect for his or her private and family life, home and communications.”²⁶

This legal instrument is complemented by the decisions of the European Court of Justice that ensures uniform application of the EU law. Since the EU is still based on the institutional treaties, it is necessary to mention Article 16 of the Treaty on the Functioning of the European Union (TFEU)²⁷ and Article 39 of the Treaty on European Union (TEU)²⁸ that deal with the data protection.

2.1.2.1 EU secondary legislation - Directives

The core EU legislation regarding privacy and data protection is the Directive 95/46/EC on the protection of the personal data (Data Protection Directive)²⁹ It is complemented by the Data Retention Directive and e-Privacy Directive.³⁰

2.1.2.2. Data Protection Directive

The Data Protection Directive is one of the most comprehensive instruments that have been published in this area. Its problem is however that it was created in 1995 and some of its articles are out-dated, particularly when it comes to electronic communications. Issues that are becoming more and more important such as behavioural (target) advertising in the new online world (such as Facebook, Google or Twitter) are difficult to be grasped within this directive. Article 29 WP is trying to supplement these deficiencies by clarifying opinions (for example the issues of consent, cookies, applicable law etc.). Since the Smart Grids functionality has a special nature, it is quite challenging to apply all data protection articles to this specific issue. Many experts (on behalf of the EC and other

²⁶CFR, article 7

²⁷C 11 5/47 The Treaty on the Functioning of the European Union. 2008.

²⁸C 115/13 Treaty on the European Union. 2008. (2007/C 306/01 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. 2007.)

²⁹See Directive 95/46/EC (Data protection directive)

³⁰There are also other EU legal instruments that mention privacy and data protection such as the Framework Decision dealing with data protection with regard to criminal matters (Council Framework Decision 2008/977/JHA) or Regulation that lie down data protection rules for EU institutions and bodies (Regulation 45/2001)

European bodies) were trying to come with an idea whether it is possible to apply the Data Protection Directive to Smart Grids/smart meters or whether it will be better to come with a sector specific solution to this problem.³¹ The current consensus in the European Commission is that specific legislation (such as new regulation) is a better option than trying to apply the current legislation to Smart Grids (will be elaborated in chapters 3, 4).³² In this context is necessary to mention that current DPD is going through a process of review and might be changed soon (so far, it seems that the revision has been postponed until 2012).³³ European Commission itself presents a list of reasons for the review of the data protection legal framework such as: challenges of globalisation or use of new technologies, free flow of personal data within the EU and beyond, improvement of clarity and coherence of the EU rules for personal data protection, consistent and effective implementation of the data protection right on the whole EU level.³⁴ “According to the most recent information from the DG Justice, the revision of the EU data protection framework will be based on four pillars: (1) the right to be forgotten, (2) transparency, (3) privacy by default, and (4) protection regardless of data location.”³⁵

2.1.2.3. e-Privacy Directive

The main focus of the Directive 2002/58/EC (the so called e-Privacy Directive) is protection of personal data that are processed in relation to e-communication networks and services. The e-Privacy Directive cannot be fully understood without consideration of the Data Protection Directive, however, it has to some extent a greater reach than the DPD (it functions as a protection against marketing). The European Commission decided to amend the whole e-communications regulatory framework in 2009. The new amended Directive 2009/136/EC (amending the 2002/58/EC Directive) should be able to protect

³¹For example: Expert Group 2 (February report, draft June 2011 report), European Data Protection Supervisor (letter to Mr. Oettinger from 27.10. 2011)

³²Keith Nuthall, *EU smart grids privacy legislation under discussion*, Utility Week, 1. July 2011

³³So far, there are no official information from the EC that the new DPD would be discussed by the end of the year. Review of the data protection legal framework, available at http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

³⁴Ibid.

³⁵Expert Group 2, draft report from 6.6.2011

users of e-communication networks and services and increase competition in the e-communications market. Since intelligent networks are partially based on ICT services and thus e-communication, this directive should be taken into account. With regard to Smart Grids/smart meters, the main implications could be to processing of the traffic data (Arts. 6 and 15), location data (Art. 9) and data breach notification (Arts. 4,5) (will be elaborated in legal analysis part).³⁶ “The implementation of Smart Grids potentially connects location information to specific data that holds information on the use of electrical energy.”³⁷ If not properly safeguarded, this personal data could be misused. To what extent can the above mentioned provisions protect the Smart Grid users will be subject of evaluation in further chapters. One should however bear in mind that telecommunications will be one of the key elements that make the grid smart.

2.1.2.4. Data Retention Directive

When discussing the EU legal framework, it is necessary to write about the Directive 2006/24/EC (the so called Data Retention Directive).³⁸ This directive caused a lot of controversies during the implementation process (it was claimed by some that it violates the secrecy of telecommunications or the human right of informational self-determination).³⁹ Even though it was published already few years ago, it was not transposed in all the Member States. Some supreme or constitutional courts have voided the national laws that implemented the Directive or declared them unconstitutional (Romania, Czech Republic, Germany). The Data Retention Directive was a reaction to the terrorist attacks in Europe, intended to become an important tool against terrorism.

The traffic data that are being collected by the providers of public communications has to

³⁶DIRECTIVE 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*) as amended by the Directive 2009/136/EC of 25 November 2009

³⁷Expert Group 2, draft report from 6.6.2011, page 5

³⁸DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (*Data Retention Directive*)

³⁹ Germany Federal Constitutional Court - Press office, *Data retention unconstitutional in its present form*, Press release no. 11/2010 of 2 March 2010, available at <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html>, accessed on November 2011

be stored (according to this Directive) for a minimum of 6 months and a maximum for 2 years. This was one of the main reasons for the controversy among EU/EEA members. There has been a fear of misusing the traffic data for other purposes and the public strongly disagreed with such measures.

The question is whether the Data Retention Directive actually applies or will apply to Smart Grids/smart metering. Its connection to Smart Grids can be seen mainly in collecting and storage of smart meters data. The February report from the Expert Group 2 has the view that applicability of specific data protection directives needs to be assessed (Directive 2002/58/EC, Directive 2006/24/EC).⁴⁰ The opinion of Art 29 WP on smart metering states that “retention policies and practices will need to be established for new purposes and reviewed for the existing purposes.”⁴¹ Since the Data Retention Directive focuses mainly on the telecommunication sector and not on the other sectors that are important in intelligent grids (such as network maintenance, taxation or value added services), its applicability to the smart metering/Smart Grids is limited.

2.2 EU legislation regarding the Smart Grids/smart meters

There are also other legal instruments that govern Smart Grids in general but these do not mention data protection or privacy issues.

2.2.1. Energy Internal Market Directive (Electricity Directive)

The Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (Energy Internal Market Directive - EIMD)⁴² is together with the Directive 2004/22/EC on measuring instruments (Measuring

⁴⁰ Task Force Smart Grids, Expert Group 2: *Regulatory recommendations for data safety, data handling and data protection*, issued 16.2.2011

⁴¹ Article 29 WP, Opinion 183, page 17

⁴² Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (*Energy Internal Market Directive- EIMD*); some sources use the term Electricity Directive, this thesis is using EG 2. title

Instruments Directive - MID)⁴³ the main legal framework for Smart Grids. Surprisingly, neither Smart Grids/smart metering, nor privacy or data protection were given much space in these legal texts (will be elaborated further).

The EIMD is part of the Third Energy Package that was approved by the European Commission in 2009. The package refers to both the electricity and natural gas sectors (Natural Gas Directive).⁴⁴ One of the main aims of the “Package” was the improvement of the functioning of the internal electricity and gas markets, effective unbundling and encouragement of modernisation of the electrical grids in Europe.⁴⁵ The EIMD refers to the introduction of Smart Grids as well as smart metering (intelligent metering system). For example recital 27 states that “Member States should encourage the modernisation of distribution networks, such as through the introduction of smart grids”...whereas recital 55 describes that if the economic assessment of intelligent metering concludes its reasonability, Member States should be able to implement the intelligent metering.⁴⁶ Also Article 3(11) states that Member States, in order to promote energy efficiency, shall optimise the use of electricity by introducing intelligent metering system or smart grids, where appropriate.”⁴⁷ The most important for the Smart Grids roll-out is however the Annex I. of EIMD that stipulates that at least 80% of consumers shall be equipped with smart meters by the end of 2020 in the case that the economic impact assessment results are positive.⁴⁸ These assessments should be finished until the end of 3. September 2012.⁴⁹ In the Natural Gas Directive are similar provisions for smart metering (intelligent

⁴³Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments (*Measuring Instrument Directive-MID*)

⁴⁴Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC

⁴⁵The package included for example higher standards of service, security of supply, efficiency gains or competitive pricing

⁴⁶EIMD, see supra note

⁴⁷EIMD, see supra

⁴⁸EIMD, see supra

⁴⁹EIMD, see supra, Annex I., para 2

metering), however since these technologies are not as developed as the electricity meters, there is no specific deadline for their implementation.⁵⁰

Even though the Third Energy Package tries to address some of the issues of data processing, there is no further guidance on privacy and data protection issues. As one can see in Article 37(1) (p) or Annex I. of EIMD the focus is on consumer rights or transparency. Consumers shall have their consumption data at their own disposal within sufficient time frame and shall be properly informed of their electricity consumption (costs).⁵¹ Consumer duties are to give any registered supply undertaking access to the metering data (by explicit agreement and free of charge).⁵²

2.2.2. Measuring Instruments Directive

Directive 2004/22/EC on measuring instruments (Measuring Instrument Directive-MID) is important mainly because its focus on electricity, gas, water and heat meters and the requirements these instruments need to satisfy.⁵³ Since this legislation was enacted prior to the Smart Grids roll-out, there is no direct reference to intelligent meters. Some of the general provisions could however be used even for smart metering purposes. For example, Member States should not impede placing of the meters on the market and should carry out conformity assessment before doing so.⁵⁴ Also Annex MI-003, paragraph 5(3) mentions the data retention of the meters: "in the event of loss of electricity in the circuit, the amounts of electrical energy measured shall remain available for reading during a period of at least 4 months."⁵⁵

⁵⁰See for example recital 52, Art. 3(8), annex I. (2) of the Natural Gas Directive

⁵¹EIMD, see supra, Annex I., (i)

⁵²EIMD, see supra note, Annex I.(h)

⁵³Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments (*Measuring Instrument Directive-MID*)

⁵⁴*Ibid.*

⁵⁵*Ibid.*

2.3 The European Union documents concerning Smart Grids

In November 2009 decided the European Commission to set up a Task Force on Smart Grids in order to support the EU roll-out of Smart Grids.⁵⁶ The first Steering Committee⁵⁷ meeting agreed on establishing of a three expert groups whose main task is to advice the Commission on policy and regulatory directions (make regulatory recommendations for Smart Grids and point out other important issues that need to be solved).⁵⁸ The second Smart Grid Expert Group task is to find proper regulatory scenario and recommendations for data protection, data handling and data security. The above mentioned group came with several reports on this issue This thesis focuses on the version from February and final draft from June 2011 since both reports come with important recommendations for the privacy and data protection in the Smart Grids/smart metering on the EU level. If those recommendations are accepted by the European Commission, the draft June report might become the future basis of a new legal framework for Smart Grids. It is thus necessary to evaluate and discuss outcomes of these reports.

2.3.1. The February 2011 report

The February report introduces definitions of data types, personal data, location data, technical data and metering ownership.⁵⁹ The Expert Group 2 suggests definition for Smart Grids and smart metering. A chapter on the current European privacy framework briefly touches the most important issues such as legal basis for data processing in smart

⁵⁶Overview of the Expert Groups of Task Force on Smart Grids: EG 1. Functionalities for Smart Grids, EG 2. Regulatory recommendations for data safety, data handling and data protection, EG 3. Roles and responsibilities of actors involved in Smart Grids deployment – available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_groups.pdf Another fourth expert group was added on the 7th Steering Committee meeting in December 2010 – EG 4. Smart Grid aspects related to gas – more information available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group4.pdf

⁵⁷This happened also in November 2009 in European Commission, Task Force Smart Grids – vision and work programme, March 2010

⁵⁸Task Force Smart Grids, Expert Group 2: *Regulatory recommendations for data safety, data handling and data protection*, Report, issued 16.2.2011, available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

⁵⁹These are more elaborated in the appendix A of the report

metering/Smart Grids.⁶⁰ The report then continues with stakeholder analysis, benchmarking of Smart Grids with other industries (banking, telecommunications, road pricing) and brief description of other countries experience (US, Dutch examples).⁶¹ This section on data privacy defines and distinguishes between personal and non-personal data and is important for further legal analysis.⁶² This was later referred to in the Article 29 Data Protection Working Party Opinion 12/2011 on smart metering.⁶³ As one can see, all the above mentioned EU documents are intertwined and try to build to some extent on each other.

The February report started an important discussion about the legal framework update, however some of its parts require deeper legal analysis. So far, it can be said that the February report is touching upon important issues that should be elaborated further. In June 2011, the Expert Group 2 presented a final draft of its report titled: *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection Recommendation to the European Commission* (currently waiting for approval).⁶⁴ On 15. June 2011, it was stated that after the summer there will be a joint meeting of the European Commission with the Expert Group 2 to identify the needs for sectorial legislation on privacy and security in the Smart Grids where the draft report will be updated and re-submitted by the end of the year.⁶⁵ According to the letter from the European Data Protection Supervisor, this meeting took place on 8. November 2011, so far no more information about this meeting is publicly available.⁶⁶ This means that if there is a need for a sectorial legislation, it will come no earlier than in 2012.

⁶⁰This part of the report comes with the first recommendation for Expert Group 2. The Group should assess if the current EU legal framework for data protection and privacy is sufficient for Smart Grids or whether is necessary to make changes.

⁶¹ Expert Group 2, February 2011

⁶²The report also includes section on data security and data handling which will not be tackled in this thesis

⁶³The Article 29 Data Protection Working Party... «will refer to research that has been carried out already by the Smart Grids Expert Group», *Opinion 12/2011 on smart metering* (from 4. April 2011), available at http://idpc.gov.mt/dbfile.aspx/WP_183.pdf

⁶⁴Expert Group 2, draft report from 6.6.2011

⁶⁵European Commission, Directorate-General Energy, Directorate B- Security of Supply and Energy Markets, *Meeting minutes from the 9th meeting of the Steering Committee of the Task Force for Smart Grids*, 15.6.2011, available at http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

2.3.2 Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection Recommendation to the European Commission

The draft report focuses on the most important issues of Smart Grids deployment in the European Union.⁶⁷ It is the most detailed document published in this area. Evaluation of its recommendations will be done in detail in chapter 4.2. The contribution of the report can be seen in thorough description of the current general privacy and data protection framework of the EU and in tackling issues that come with Smart Grids and smart metering functionalities. It deals specifically with privacy in Smart Grids which has never been the case before (in other EU documents). Among other interesting topics are data retention, security in Smart Grids, cyber security. In the appendices, outcomes from other expert groups are included. The main recommendations from the Expert Group 2 are presented in executive summary in the beginning of the report.

For the purpose of this thesis it is necessary to briefly focus on the Article 29 Working Party that published important opinions – one on the smart metering and one on consent.⁶⁸ Both these issues play crucial role in Smart Grids deployment. Even though the Art. 29 WP does not represent a binding legal source, its opinions can be seen as important guidance when there is no further guidance from the courts (this does not mean that opinions are widely accepted by legal professionals). Thus is necessary to critically discuss those opinions before further legal analysis is made.

⁶⁶European Data Protection Supervisor, Letter from Assistant Supervisor to Mr Günther Oettinger, Commissioner for Energy - *Proposal for a Directive of the European Parliament and of the Council on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC*, 27.10.2011

⁶⁷Task Force Smart Grids, Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection- final draft*, issued on 6.6.2011

⁶⁸Article 29 Working Party: Opinion 12/2011 on smart metering, 4 April 2011 (Opinion 183 on smart metering), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf and Article 29 Working Party : Opinion 15/2011 on the definition of consent, 13.July 2011, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

2.3.3. Article 29 Data Protection Working Party documents

The Article 29 Data Protection Working Party (further referred as Art.29 WP) was set up by the Data Protection Directive (Directive 95/46/EC).⁶⁹ It regularly comes with expert opinions on issues regarding data protection. In 2011 came Art. 29 WP with some of the most relevant documents for the Smart Grids problematic (opinion on smart metering and opinion on the definition of consent).

2.3.3.1 *Opinion 183 (12/2011) on smart metering*⁷⁰

The Expert Group 2 from the Task Force on Smart Grids asked the Art. 29 WP for analysis of smart metering measures in the EU Member States. The smart metering opinion did not include Smart Grid functionality, but it did not rule out further analysis of Smart Grids completely. Parts of the report were based on answers from Data protection authorities (DPAs) that received a set of questions regarding Smart Grids and smart metering implementation. The Working Party realised that due to the differences across the EU Members states it was not possible to provide more specific recommendations in this area. As is written in the opinion from April 2011, the Art.29 WP analysis focused on the “relationship between the legal requirements set out in the Data Protection Directive and the context of the smart metering”⁷¹ and also referred to the work of Smart Grids Expert Groups. A thorough examination of their presented results (as for example applicability of data protection law to smart meters) will be done in chapter 3.1. Some of the main issues that were touch upon are: definitions, data controllership, data processing, consent, contract, legitimate interests, privacy by design, personal data retention, third parties and data security. The main outcome of this opinion is inter alia the fact that data protection laws will apply to the smart metering since personal data are being processed.

⁶⁹More details on the task of the Article 29 Working Party can be found on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/tasks-art-29_en.pdf

⁷⁰Article 29 WP: Opinion 183 on smart metering

⁷¹Article 29 WP: Opinion 183

2.3.3.2. *Opinion 15/2011 on the definition of consent*

The 12/2011 opinion on smart metering touched also upon the issue of consent. Consent is one of several legal grounds for processing legal data thus an important part of the DPD.⁷² Relevancy for smart metering lies in the explanation of the valid and invalid consent. The 15/2011 opinion presents examples of situation where consent is/is not freely given. Interesting parallel with smart meters can be seen with the example of electronic health records (page 15). If there is no other option for the service to be provided, refusal means a clear disadvantage for people who will not consent. The Art. 29 WP thus came to the conclusion that consent is not sufficiently free in the case of electronic health records.⁷³ If we think of smart meters, the option not to install smart meters might mean that the household will not be provided electricity, gas, water etc. Is this considered to be an option for those not consenting? From the similar perspective as the opinion on consent, one can conclude that consent is not sufficiently free (in the case of smart meters), if there is no option.

This chapter presented in a nutshell the legal framework that needs to be considered in the Smart Grids environment. To what extent are these instruments sufficient legal framework for the new intelligent grid will be discussed in chapter three and four.

⁷²Article 29 WP : Opinion 187

⁷³Ibid.

3. Legal analysis

In order to determine whether the European data protection framework (more specifically, Data Protection Directive) applies to smart metering/Smart Grids, a question needs to be asked whether personal data are being processed by the means of intelligent metering. Personal data means that data can be related to a natural person (according to Art.2 DPD personal data shall mean any information relating to identified or identifiable natural person – data subject).⁷⁴ For the Smart Grid purposes technical data (any data necessary for the maintenance of the grid) are also processed. Expert Group 2 remarks that technical data could also be personal data.⁷⁵

3.1 Data processing

Article 29 Data Protection Working Party gives us guidance on data processing in its opinion 183. Even though this text is not legally binding, we can assume that courts might tend to the same interpretation as the experts from the Art. 29 WP. In the Opinion 183 a list of data types that are expected to be processed is presented:

- *"Unique smart meter ID and/or unique property reference number (even in the absence of these identifiers, the meter might also be identified by its unique energy load graph);*
- *Metadata referring to the configuration of the smart meter;*
- *A description of the message being transmitted, for example whether it is a meter reading or a tampering alert;*

⁷⁴DPD, Article 2

⁷⁵EG 2 defined technical data in its February 2011 report as follows: "This data should not be able to be linked to individuals or households, as long as this data is not gathered on an individual supply point level (as in a household or a charging pole). When this data can be linked to a person it is also personal data and rules regarding personal data should apply." http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf in Expert Group 2, draft report from 6.6.2011, page 55

- *A date and time stamp;*

- *Message content.*"⁷⁶

This shows us for example that if meter ID is given to a specific consumer that can be recognized by the grid operator, the data are then being considered as personal. As the Task Force on Smart Grid concludes, the main question is whether it is possible to design the smart metering technology in a way that avoids involving personal related data.⁷⁷

Since one of the main arguments of Smart Grid creators was that people can see their own consumption in real time and can thus control it more effectively, one needs to ask whether it is possible to get these data in a different way, excluding links to an identifiable natural person. If no personal data are involved, there is no privacy or data protection issue to be solved and the data protection framework would not apply. The Task Force Smart Grids Expert Group 2 (in its Recommendation to the European Commission from June 2011) stressed that whenever possible, Smart Grids operation should be based on non-identifiable data.⁷⁸ We can ask ourselves how would this be translated to reality. The possibilities of data anonymisation or data aggregation are currently being evaluated as limited (will be presented in further chapters). Thus it seems that smart metering based on non-identifiable data is currently not the option (possible) unless researchers come with new enhanced method of data collection.

So far it can be said that personal data are contained in the information generated and disseminated by smart meter. The Art.29 WP determines that the Data Protection Directive applies to such processing.⁷⁹ The opinion 183 presents three main reasons for such conclusion – 1) individuals can be recognized from other consumers if they are

⁷⁶ "Message content is likely to include the following types of information: - Meter register read. This could be a single reading or a group of readings for a more complex tariff; Alerts. The meter may transmit a message informing that an event has triggered the meter's alarm; Network level information such as voltages, power outages and power quality; Load graphics with various levels of detail." in Art. 29 WP, opinion 183

⁷⁷ Task Force Smart Grids, Expert Group 2: *Regulatory recommendations for data safety, data handling and data protection*, Report, issued 16.2.2011

⁷⁸ Expert Group 2, draft report from 6.6.2011

⁷⁹ Art. 29 WP, Opinion 183

using smart meters (unique identifiers are linked to the living individual who pays the bill); 2) consumer's energy profile can be used/utilised for decisions directly affecting him/her; 3) the success of smart meters lies in reducing individual energy consumption which requires collection of large amounts of personal data from consumers (which is necessary according to energy suppliers).⁸⁰ The third issue has no clear cut answer, currently, there is no other option for reduction of overall energy consumption than to collect personal data and thus make people aware of their energy use. Therefore, it is necessary to presume that personal data will be needed (at least for some time) for the success of smart meters. Given the current situation, there is no sign that intelligent meters will be working solely on the basis of non-personal data (this would go against the original purpose that people would be aware of their own energy consumption). This thesis can thus conclude that since personal data are processed in smart meters, the European data protection framework applies to Smart Grids/smart metering.

3.2 Distinction between data controller and data processor

Before going further, it is important to make a distinction between data controller and data processor since the former has many legal obligations under the data protection legal framework.⁸¹ According to the DPD, data controller is "the natural or legal person, public authority, agency or any body which alone or jointly with others determines the purposes and means of the processing of personal data.." whereas data processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."⁸² Since it is not always easy to distinguish one from the other, the Article 29 Working Party came with a clarifying opinion 1/2010 on this issue.⁸³

⁸⁰Art. 29 WP, Opinion 183

⁸¹According to the Data Protection Directive, data controller has to be responsible for compliance with DPD rules. There are also number of provisions where is necessary to distinguish who is data controller and who data processor (applicable law, data subject, data protection authorities)

⁸²DPD, Art. 2 (d)

⁸³Art. 29 WP, *Opinion 1/2010 on the concepts of "controller" and "processor"* (Opinion 169) from 16.2.2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf - – an interesting parallel to the Smart Grids data controllers could be seen in the example of Telecom operators who are considered controllers "in respect of the processing of the additional personal data necessary for the operation of the service" - but only for traffic and billing data

Current situation enables parties to be a data controller in one country and a data processor in another country. There are different actors in the energy sector such as the distribution system operator (DSO), transmission system operator (TSO), energy supplier, regulatory or government bodies, communication and third party providers (and many others). Art. 29 WP describes in detail in what circumstances can be those parties considered data controllers:

- 1) DSOs (or network operators) – as a grid owner, DSO is responsible for installation and running of the smart meters and thus determines how the data are collected, stored and used.⁸⁴ In this scenario the DSO is the data controller.
- 2) Energy suppliers – if they use the meter data for their own purposes (billing, advice) or have contract with the data subjects; the Art. 29 WP holds the view that ”suppliers remain a data controller...notwithstanding the added complexities brought about by smart meters.”⁸⁵
- 3) Other parties can be considered data controllers when fulfilling the following: energy regulators if they have access to personal data for policy setting and research purposes; third party service providers if the personal data are disclosed for the purpose of providing a service (to consumer, energy supplier); certain communications function deciding on enclosing personal data to third parties or re-purposing of such data.⁸⁶

In the case of smart meters, the most common case is that in one Member state could be the data controller the DSO that owns the grid and in the second member state is the data controller the energy supplier. More specifically, in most EU countries lies the responsibility for administration of data with the DSO, exception being UK and Germany where energy suppliers are likely to be responsible for administering most meter level

⁸⁴ Art. 29 WP. Opinion 183

⁸⁵ Ibid.

⁸⁶ Ibid.

data.⁸⁷ It is also necessary to bear in mind that when data is being processed by multiple actors this can be considered as a joint control.

3.3 Requirements for the processing of personal data

Since the previous chapter showed that the European data protection framework applies to Smart Grids/smart metering, one has to assess whether there is a need to prepare specific legislation for Smart Grids. An analysis of the current data protection rules will be used in order to determine the necessity of additional legal basis.

If we presume that personal data is processed via smart meters, according to the Article 6 of the EU Data Protection Directive: “Member States shall provide that the personal data are processed fairly and lawfully...collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes.”⁸⁸ Fair and lawful processing that can be found in Article 6 (1)(a) and data minimization principle found in Article 6 (1)(b) and (c) as well as purpose limitation are among the basic principles of data protection. Data quality is another essential criteria as can be seen in Article 6 (1) (c): the data processing shall be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed” or Article 6 (1) (d): “accurate and, where necessary, kept up to date [...]”⁸⁹ One of the most important of those principles is the data minimization principle (an effort to use as minimum personal data as possible during the data processing). Smart metering/Smart Grids is on the contrary based on collecting more information on customers than before (for energy efficiency purposes). The main aim is to improve electricity consumption awareness among consumers. The data protection legislator’s goal should be however the reduction of the data collection to essential/non excessive data that can be used for Smart Grid purposes. We can also assume that operators would be willing to offer other

⁸⁷Expert Group 2, draft report from 6.6.2011

⁸⁸DPD, Article 6

⁸⁹DPD

services via third parties. Those involved will be trying to get as much data as possible since this information is valuable for example for target advertising. This all goes against the principle of data minimisation, one of the main criteria of the EU data protection framework.⁹⁰

Notwithstanding the problems with the former principle, smart metering data processing could be still considered legitimate (for reasons such as improvement of energy efficiency, grid stability, accuracy of metering). Data Protection Directive however requires also other principles to be fulfilled to legitimise processing of the data. These are described in detail in Article 7:

"...personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)." ⁹¹

The legitimate basis requires deeper analysis since each of these criteria can be questioned in the case of Smart Grids. Article 29 Working Party in its Opinion 183 states that the exact nature of the purposes for the processing of personal data from smart meters has yet to be made absolutely clear or properly defined.⁹² It also warns about

⁹⁰The principle of data minimisation (Art. 6(b)-(c) of the 1995 DPD

⁹¹DPD, Article 7

⁹²Art. 29 WP. Opinion 183 on smart metering

reprocessing of personal data for other purposes incompatible with the original collection of personal data.

Before answering the question whether it is necessary to prepare specific legislation for Smart Grids, each of these principles will be evaluated in detail.

3.4 Data subject consent

Consent is one of the several legal grounds for processing personal data.⁹³ Even though it has an important role, there are also other legal grounds that can be sometimes considered more appropriate than consent (will be elaborated further). Consent gives the data subject control over processing of own data, however one needs to be careful. There are number of questions that have to be tackled such as whether consent is unambiguous, free, explicit, specific or informed. An unambiguous consent can be revoked at any time (sometimes without any reason). This can be problematic in the case of Smart Grids since we have to distinguish between personal data processing for the purposes of energy supply (production, transmission and distribution) and for value added services (any other services than energy supply).⁹⁴ As Expert group 2 suggests in its report, "concerning the former purpose, in case smart metering is voluntary, processing of personal data should be based on consent; otherwise - processing shall be required by law...concerning the latter purpose, processing shall always be based on an unambiguous consent, separately given for each value added service (i.e. 'opt in' regime)."⁹⁵

It will be important to educate people about implications of smart metering consent. Smart Grids transmission cannot exist under uncertainty, this would hamper the security of energy supplies which one wants to avoid. In the case of value added services, it is understandable that the opt in regime was chosen by the Expert Group 2. People could be flooded by many different suggestions for services and the opt-out regime would not be

⁹³Art. 29 WP, Opinion 187 on consent

⁹⁴Expert Group 2, draft report from 6.6.2011

⁹⁵Ibid.

convenient for them. Especially when considering the current practices (such as target advertising or IT services where consent is necessary in order to be able to receive the service). There should be a careful evaluation of the possible wording of such opt-in regimes (separate analysis for this purpose is needed). Expert Group 2 also suggests that consent can be withdrawn free of charge any time, taking into account contract law.⁹⁶ This move is understandable in the case of added value services and should be supported.

Article 29 Data Protection Working Party in its opinion 183 reminds that a fully-informed decision is the main precondition for a valid consent (data subject needs to be given sufficient information about the personal data processing to make a genuine choice).⁹⁷ It is however questionable whether this will be enough for the consumers to be able to make a genuine choice. If consent will be the precondition for some of the basic Smart Grid functionalities, people will tend to consent in order to be provided electricity. Is consent the right legal tool for smart metering? Its advantages are that people can decide themselves about the provided service. However, there is still a question to what extent will be the consent sufficiently informed and free. Art.29 WP states that data subject should be able to change his/her consent "without going to excessive amounts of trouble" and suggests designing of the "household control panel to include 'push button' consent."⁹⁸ To be critical, this offered solution might be hampering the Smart Grids functionality. If consumers agreed to some kind of service and suddenly withdraw their consent, the electricity transmission might not be that stable. To conclude, consent has number of weaknesses yet to be properly evaluated – it can be revoked any time, it must fulfil a number of legal preconditions (whose implications are not yet solved). Those who draft the legislation need to consider carefully whether consent is better suited for smart metering/Smart Grids than other legal grounds. If however, there is no other tool for permission of data processing within this framework, consent should be considered as an option.

⁹⁶Expert Group 2, draft report from 6.6.2011

⁹⁷Art. 29 WP, Opinion 183

⁹⁸Ibid.

3.5 Contract

Consumers usually enter into more contractual relationships with players in the energy supply market.⁹⁹ If the data controller fulfils obligation which was agreed between data subject and controller in a contract, data processing can be legitimate. Implications of the performance of contract are in detail discussed in article written by Knyrim and Trieb.¹⁰⁰ Below examples of processing that is necessary for contract will be presented. Firstly, distribution system operator (DSO) needs to sustain a certain level of stability and security of the grid which is becoming more complicated with the rising demand and diversification of energy sources. Since smart metering offers a quicker reaction to energy supply shortages, processing of intelligent meter data “could be justified by its necessity for the performance of contractual duty”.¹⁰¹ One can however argue whether ensuring the grid stability needs personal data processing. Secondly, the energy suppliers will need detailed data about energy consumption in order to be able to bill customers for specialised tariffs. They will need this data from the DSOs (data controllers). Contractual duty between customers and energy suppliers could be, therefore, problematic since the Article 7(b) of the DPD legitimises only performance of the contract between data controller and data subject as Knyrim and Trieb suggest.¹⁰² The energy supplier will be in this case considered a third party. Third parties have different legal regime than the data controllers. Knyrim and Trieb argue, however, that transfer between these two parties is legitimate if it is necessary for a third party to fulfil contractual duty towards the data subject.¹⁰³ It is important to stress that customers could be deprived of their chance to contract with energy suppliers, if this argumentation would not be accepted.¹⁰⁴

We can see a clash between the different approaches where data protection supporters would stress that processing as well as the transfer of data on the basis of the

⁹⁹It is usually two or three separate contractual relationships

¹⁰⁰Knyrim, R., Trieb, G., *Smart metering under EU Data Protection Law*, International Data Privacy Law, 2011

¹⁰¹Ibid.

¹⁰²Ibid.

¹⁰³Ibid.

¹⁰⁴Ibid.

performance of a contract is only lawful to the extent absolutely necessary¹⁰⁵ whereas people who are not that concerned with those issues would be stressing the importance of undisturbed service. One can agree with Knyrim and Trieb who are questioning the necessity of collecting metering data in 15 minutes intervals for energy supplier purposes. Usually, energy suppliers prepare some offers that can be used by bigger percentage of customers; it is highly unlikely that each customer will have their own personalised offer. In such case it is most probable that consumers could choose from a few/dozen tariff options where such a detailed (15 minutes intervals) might not be necessary. If, however, energy suppliers insist on having such elaborated data, this should be taken into account when preparing further legal framework.

In the end, this will depend on the agreement between DSOs and energy suppliers. The important fact for the customer is that both contract and consent give him/her some legal options in the case of smart metering roll-out. It is, however, clear that more precise rules need to be established. Further discussion of this issue will be presented in following chapter.

3.6 Legal obligation

The strongest legal basis for data processing from smart metering could come if a legal provision (such as regulation) is enacted on the European level. Even though there are currently some discussions about this possibility, it is now up to the Member States to provide legal foundation for Smart Grids. The Electricity Directive needs to be implemented into national laws and, therefore, we can witness quite different approaches towards smart metering.¹⁰⁶ For example in some EU countries, “the network operator has the obligation of installing and collecting data through smart meters for every new installation.”¹⁰⁷ In Italy, a number of smart meters have been already installed.¹⁰⁸ Other countries have only slowly started with legislative efforts. We also need to bear in mind

¹⁰⁵Knyrim, R., Trieb, G., *Smart metering under EU Data Protection Law*

¹⁰⁶National Statutes mandating the implementation of smart metering have been enacted in Italy and Sweden in Knyrim, R., Trieb, G., *Smart metering under EU Data Protection Law*,

that most of those countries are fulfilling the aims of the EIMD which lacks provisions on privacy or data protection. For a national statute to be passed, it is necessary to fulfil applicable legal requirements of the Article 8 of ECHR (this will in detail discussed in chapter 3.10).¹⁰⁹ As was shown above, data processing for compliance with a legal obligation of the controller would create the strongest legal basis for smart metering, it would be however very complicated to come with a proposal that everyone would agree on.

3.7 Legitimate interests

Data processing could be also justified under Article 7(f) of the DPD as the legitimate interests pursued by the data controller or by a third parties.¹¹⁰ These interests can for example be maintenance of the grid by the DSO (ensuring the grid stability) or increased efficiency in energy supply. Important point is, however, made by the Article 29 Working Party which stresses that even though some personal data use seems legitimate, that “does not mean that it can be applied to legitimise every element of processing.”¹¹¹ For example, even if the efforts to increase energy-efficiency seem to be justifiable in a sense of common good, data controllers should not be able to get intimate details from the data subject (this means that legitimate interests of controllers cannot outweigh the fundamental rights of data subjects). Particularly when the controllers actions are too intrusive or cause detriment to the data subject. In the case of third parties legitimate interest is questionable and would probably be refused.

¹⁰⁷For example the French decree no 2010-1022 of August 31, 2010 in Article 29 Data Protection Working Party, *Opinion 183 on smart metering*, 2011

¹⁰⁸Joint Research Centre, *Smart Grid projects in Europe*

¹⁰⁹According to Knyrim and Trieb: Any legislation will need to provide: indication for the scope and conditions of the data processing; determination of the possible group of data subjects; regulations prohibiting certain kinds of comments of the personnel of the controller with regard to the data of the data subjects processed; regulations with the regard to the legitimacy of the storing of information or data deletion in *Smart metering under EU Data Protection Law*

¹¹⁰DPD, Article 7(f)

¹¹¹Article 29 WP, Opinion 183

Practical applicability of the Article 7(f) needs to be evaluated in each case by data controllers. Privacy impact assessments and privacy enhancing technologies that could increase data protection, might also help with the application of this provision (Art.7 (f) of DPD). Controllers would have a reason to say that since personal data have a better protection, their (society's) legitimate interests of increased efficiency in energy consumption are justified.

3.8 Data retention

Smart metering poses new challenges to data retention (data storage). The enormous data collection that is expected to be provided by intelligent meters must be taken into account by the authorities. A review of the existing policies on data retention is needed. It must be noted that the Data Retention Directive from 2006 is applicable mainly to telecommunications whereas Smart Grids encompass a much wider area.

As can be seen in the Article 6(1) (c) of the Data Protection Directive, data should be kept only for a limited period of time (necessary to fulfil purposes of their collection).¹¹² The principle of data minimisation is important to keep in mind. There are also other factors that need to be taken into account such as transparency (who, when and under what circumstances retains the personal data; what data and where it is stored) or consumer empowerment (safeguarding consumer rights).¹¹³ Data retention (collection) should not exceed the absolute minimum. In the case of Smart Grids, there are a number of different purposes for data collection. To mention some of them: billing, taxation, network maintenance, value added services, law enforcement or political aims.¹¹⁴ Data retention periods can, however, differ a lot according to the different rules in the Member States. If we take for example taxation, here the length of the compulsory data retention

¹¹²DPD, see supra note

¹¹³Expert Group 2, draft report from 6.6.2011

¹¹⁴This thesis is using the same purposes as the Expert Group 2 draft June report for a better understanding of the table with suggested data retention periods that is below. For a thorough analysis of different data retention purposes, please see pages 35-39 of this report.

could vary from 3 years in the United Kingdom to 10 years in France.¹¹⁵ Bills for electricity are also processed and sent to the customers according to the Member States procedures and habits. Experts from the EU institutions however came with proposal for the billing retention period that could suit all (customers and utilities). Article 29 Working Party suggests that thirteen months may be appropriate time period for data retention to achieve a specified and lawful purpose of the data controller (for example billing and payments or provision of energy efficiency advice).¹¹⁶ This means that for normal billing, utilities should be able to work with yearly data. To what extent will be the offered period accepted across the EU Member States remains a question. One should agree that this is reasonable. In the case that customer would like to complain about its own bills a longer storage period should be enabled.

Before a widespread installation of smart meters, it is necessary to solve the question of data storage (the actual place where the data are stored). Usually, this would be at the utility which provides electricity (for the conflict resolution purposes). When it comes to the previous issue of billing – customers could also have the data stored on their own meter. Article 29 Working Party claims that this would “allow the data subject to make their own decisions regarding the retention.”¹¹⁷ In any case, the security of the data must be guaranteed.

To provide unified answers in the case of Smart Grids data retention is not easy. Expert Group 2 came with own recommendations concerning the latter. It is above the extent of this thesis to be able to thoroughly evaluate the offered retention periods (since it contains references to criminal and civil law).

Below can be found a table with suggested data retention periods for specified purposes:

¹¹⁵Expert Group 2, draft report from 6.6.2011, page 36

¹¹⁶Article 29 WP, Opinion 183

¹¹⁷Ibid.

Purpose	Scope	Length	Kept by
Network maintenance	Personal/anonymised/aggregated	strictly necessary / national law	Utility
Billing and payments	summed up usage	around 12-13 months	Utility and energy market supplier
Billing complaints	detailed personal data	national law	consumer
Taxation – tax records	summed up usage	national law	utility
Taxation – tax breaks	detailed personal data		consumer
Value added services	upon consent	upon consent	any interested
Policy making	anonymised/aggregated	unlimited	public authorities

Source: Task Force Smart Grids, Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection*, issued on 6.6.2011 – draft report

3.9 Third parties processing of personal data (value added services)

One of the concerns of the legislators are the value added services in the Smart Grids. These are usually provided on a commercial basis (either by utilities or contracted third parties). We can only imagine the range of services that could be provided for customers based on the personal data (from the energy consumption advisers to pizza delivery for people that are at home). The protection against such practices can be, to some extent, found in the e-Privacy Directive. Its Article 9 deals with location data:

“Article 9 (1): ...The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

Article 9 (2): ‘Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.’¹¹⁸

One can see that these provisions offer the consumer a choice, but only for the location data. Customers should have a much higher protection – such as opt-in for the services they want and possible withdrawal of their consent.

As was stressed many times in this thesis, one of the main concerns about the smart metering is profiling (target advertising). Profiling can be defined as “an automatic data processing technique that consists of applying a ‘profile’ to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.”¹¹⁹ When the British Government conducted a research about Smart meters, most of the respondents answered that they do not mind that their personal data will be used by utilities, but their main concern was about being flooded by different target advertising campaigns (without their explicit consent).¹²⁰ The financial profits that could be made from trade with energy profiles need to be taken into account. Legislative bodies should focus on collective action against intrusive marketing. As the Article 29 Working Party stated “it would be unacceptable for third parties to be processing detailed information about a data subject’s energy usage without the knowledge and consent of that data subject.”¹²¹

Currently, there is no specialised legislation that would cover all the aspects of profiling in the intelligent grids. The e-Privacy Directive is trying to tackle some of those issues, but it cannot be considered sufficient for the needs of smart metering. An EU wide

¹¹⁸DIRECTIVE 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*) as amended by the Directive 2009/136/EC of 25 November 2009

¹¹⁹Expert Group 2, draft report from 6.6.2011

¹²⁰Department of Energy and Climate Change, *Smart Metering Implementation Programme – A call for evidence on data access and privacy*, August 2011

¹²¹Article 29 WP, Opinion 183

regulation could be one of the ways how to prevent unprecedented business with energy profiles.

3.10 Privacy in the smart metering

This thesis will briefly look at privacy implications of smart metering. First and foremost it must be made clear from the beginning that privacy and data protection does not mean the same (while closely linked, these terms are not identical). Privacy has been defined differently by various scholars (see below). Debates about which definition is most correct are ongoing, it also depends on the region where they originate from (US, Europe).¹²² Concept of privacy was first presented in the article written by Luis Brandeis and Samuel Warren “The Right to Privacy” as a “right to be let alone”.¹²³ Different interpretation can be found in Westin’s work “Privacy and Freedom” where privacy tends to be conceived as a form of autonomy – i.e “one’s ability to control the flow of information about oneself.”¹²⁴ Gavison and Bygrave are describing privacy as a “state of limited accessibility.”¹²⁵ The above mentioned overview is not exhaustive. The most suitable definition for the smart metering case seems to be the one of Westin, about informational control, who states: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”¹²⁶ Such definition can also be applied to the reality of intelligent metering (for example in a following way): depending on the “smartness” of the meters (how), it will be possible to collect enormous amount of

¹²²More details can be found in the articles Solove, Daniel, *Understanding Privacy*, Harvard University Press, Cambridge, Massachusetts 2008 or Bygrave, Lee, *Privacy and Data Protection in an International Perspective*, Stockholm Institute for Scandinavian Law, 2010

¹²³ Warren, Samuel, D. and Brandeis, Luis, D. , *The Right to Privacy*, Harvard Law Review, 1890, p. Vol.4 No.5.

¹²⁴Bygrave, Lee, *Privacy and Data Protection in an International Perspective*, Stockholm Institute for Scandinavian Law, 2010

¹²⁵Gavison claims that privacy is a condition of “limited accessibility” consisting of three elements: “secrecy” (“the extent to which we are known to others”), “solitude” (“the extent to which others have physical access to us”), and “anonymity” (“the extent to which we are the subject of others’ attention” in Bygrave, Lee, *Privacy and Data Protection in an International Perspective*, Stockholm Institute for Scandinavian Law, 2010

¹²⁶Westin, Alan, F., *Privacy and Freedom*, Atheneum, New York 1970

personal information (to what extent) on 15 minutes basis (when) from the very sacred inside of our homes. If we would not be able to influence smart meter roll-out in any way (such as to stop installing the smart meters on data subjects premises), this could be considered as a breach of the inviolability of the home and respect for family life.

Challenges posed by smart metering to privacy must be carefully evaluated. So far, the legal analysis considered mostly data protection implications of smart metering.¹²⁷ Even though privacy and data protection issues are many times intertwined, this thesis tends to agree with interpretation that “data protection is increasingly being treated in European law as a set of rights that are separate to the more traditional right to respect for privacy or private life.”¹²⁸ As can be seen in the legal instruments mentioned in the previous chapter, the distinction is clearly made (for example in Article 7, 8 of CFR). CFR is an example of the fact that EU recognized data protection as a fundamental right itself. In order to answer the research question “whether the European data protection framework apply to Smart Grids” is, however, important to include also the privacy aspect of smart metering.¹²⁹

Chapter 2.1.1 briefly stressed that the right to privacy is usually tested by privacy test. We will now evaluate whether current smart metering framework satisfy the criteria of Article 8 ECHR (or case law of EctHR) in the terms of legality, necessity, proportionality and legitimacy.¹³⁰ For a better understanding wording of Article 8 is repeated:

“1. Everyone has the right to respect for his private and family life, his home and correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the

¹²⁷The Expert Group 2 June draft report analyses privacy in the smart metering which has usually been omitted in other similar documents presented in Europe. The report presents practical overview of the concepts of privacy and data protection on pages 20-23.

¹²⁸Bygrave, Lee, *Privacy and Data Protection in an International Perspective*

¹²⁹People tend to confuse terms privacy and data protection therefore is necessary to explain it in a special chapter. And thus clarify some of the problematic issues

¹³⁰CFR contains the same criteria as ECHR (legality, necessity, proportionality and legitimacy) but requires additionally that any interference must respect the essence of those rights and freedoms - taken from the EG 2draft June 2011 report

*economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.*¹³¹

Legality, described in the Article 8 as “in accordance with the law”, can be found in the current legal framework for smart metering (Energy Internal Market Directive and Measurements Instrument Directive). These two directives, however, focus on internal energy market, technical issues or consumer rights, rather than on privacy. Expert Group 2 in its June report states that “privacy and data protection is insufficiently regulated [concerning the current provisions of the EU smart metering framework] and [...] moreover, there is a risk of insufficient protection of privacy rights due to fragmented legislation.”¹³² The lack of privacy safeguards in the above mentioned framework could be improved by adopting a new regulation with an EU wide application.

The next step in the privacy test is the necessity “necessary in the democratic society” and proportionality criteria (both closely related). To what extent do we need smart metering in our society? Energy-efficiency and pressing climate change issues are important factors that should be taken seriously. On the other hand measures supporting wiser energy consumption should be proportionate. With a planned roll-out (80% households in 2020 equipped by smart meters) is questionable whether customers will be guaranteed free choice of intelligent meters. The freedom of choice is an important criteria of privacy (part of one’s private life). As can be seen in the example of the Netherlands, which is in detail presented in the footnote, consumer groups claimed that the proposed compulsory installation of smart meters is against the Article 8 (not necessary in a democratic society).¹³³ Government was then pressed to change the

¹³¹European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 (ECHR)

¹³²Expert Group 2, draft report from 6.6.2011

¹³³Example of the Dutch approach towards smart metering: Politicians in the Netherlands came with the idea of compulsory installation of smart meters in households. The proposal was rejected by consumer organisations and privacy groups who campaigned against the bill. Some of the suggested measures for support of smart meters roll-out was for example fine up to 17 000€ or six months in prison for not installing intelligent metering system. The Dutch Data Protection Authority was also critical to the proposal, stating that it did not comply with the Dutch Data Protection Act; some critics also suggested that such a proposal could contravene Article 8 of the European Convention on Human Rights. After the public discontent, the Dutch authorities decided that the smart meter installation will be voluntary. The amended draft of the Bill was sent to the Senate that approved the legislation on February 2011. Some of the changes consist in: customer consent for network operators access to smart meter information, remote reading of the meters consumption overview(maximum of six times a year – if customer switches provider or moves to another location).When obtaining the consent of consumer, provider

controversial bill. The right to privacy outweighed the environmental and financial arguments of legislators. To be able to opt for an old “dumb” meter instead of the smart one is the possibility that gives more space to privacy. Even though it might threaten the overall aim of the smart meters roll out, the breach of privacy is a serious concern that needs to be taken in mind. To raise people’s awareness of Smart Grids and leave them the freedom of choice could be the first step towards a successful implementation of smart metering.¹³⁴

The last step in the privacy test is the assessment of the legitimacy criteria. The latter is presented in Article 8 (2) such as “interest of national security, public safety the economic well-being of the country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others.”¹³⁵ The “economic well-being of the country” criterion seems to be the most suitable for intelligent meters. So far, there is however no evidence that smart metering would guarantee economic well-being (even though politicians presume that it could happen). Countries should, therefore, accelerate their privacy impact assessments that would help to evaluate economic and privacy aspects of smart metering. To sum up, Member States should be able to justify that smart metering interference with privacy is legitimate.¹³⁶

When trying to evaluate whether current smart metering framework satisfy the criteria of Article 8 ECHR (legality, necessity, proportionality and legitimacy) one has to say that there is still work to be done. It is also important to mention that in case of a lack of EU-wide regulatory scheme for Smart Grids (metering) national laws should ensure conformity with privacy (being a uniform standard of ECHR and CFR), especially or

might have additional access to the meter. - information taken from: International smart meter rollout sparks privacy concerns, Privacy Laws&Business International Newsletter, December 2010; <http://www.telecompaper.com/news/dutch-parliament-approves-smart-meters-legislation>, accessed on October 2011

¹³⁴The draft June report comes with own suggestions: “In order to fulfil the criteria of necessity and proportionality, the following questions are useful: 1) is (a given solution of) smart metering necessary in a democratic society? 2) is this interference proportionate to the aims pursued? 3) is there any less intrusive (onerous) solution?” in EG 2, report 6.6.2011

¹³⁵Article 8 ECHR

¹³⁶One needs to bear in mind that states have some margin of appreciation (the range of discretion) which enables them to have to some extent cultural, historic and philosophical differences.

before such a scheme enters into force.¹³⁷ There is a need to find balance – on the one hand enable the smart metering roll out while on the other hand ensuring the fundamental human right to privacy.

¹³⁷Expert Group 2, draft report from 6.6.2011

4. Recommendations on Smart Grids/smart metering and data protection

"If privacy is addressed at the design phase of the Smart Grid ("Privacy by Design"), it is possible to derive user and business friendly solutions."¹³⁸

Smart Grids present legislators with a number of challenges, privacy and data protection being only part of this complex issue. It is not easy to come with one simple solution tailored to the specific needs of the intelligent network. A number of possibilities are currently being presented and discussed and only some of them seem to be on the right track. The view shared by many experts (for example EG 2) is that current data protection legislative framework might not be enough for the protection of privacy and personal data of its users. There might be a need for technological solution that would help enhancing data protection in the Smart Grids/smart meters. One can for example look how the film industry has been dealing with copyright infringement. The legal framework was not capable of preventing illegal downloading and copying of DVDs, so the companies came with a digital rights management system (DRMS), tool for copyright holders for limiting the illegal use of digital content. This is an example of technological measure capable of fighting technological problems posed by the internet environment. Not only DRMS itself but also its legal support in some of the European Directives or Digital Millennium Copyright Act (US Act) helped to tackle copyright infringement. One needs to bear in mind that the combination of different tools is often more effective. Also Smart Grids could use solutions based on Privacy by Design (default) or privacy enhancing technologies. To what extent are these applicable to the intelligent network will be evaluated in this chapter. The main question considered is to what extent can be Privacy by Design/Default the right solution to the privacy and data protection issues in Smart Grids? What other options could help with protection of personal data in the intelligent networks?

¹³⁸Expert Group 2, report issued on 16.2.2011

4.1 Privacy by Design (privacy addressed at the design phase)

Privacy often comes too late in the IT projects. In 2009, Article 29 Data Protection Working Party published its Opinion 168 on the Future of Privacy where it suggested that "services and technologies which rely on the processing of personal data should be designed with privacy by default settings."¹³⁹ To include privacy requirements early in the development of technology, the so called "Privacy by Design", is a concept known since the 1990s. It was presented by a Canadian Privacy Commissioner Ann Cavoukian as follows: "embedding privacy proactively into technology itself – making it the default."¹⁴⁰ We first look at this concept generally and then focus on its applicability to Smart Grids. According to Ann Cavoukian, there are 7 foundational principles of Privacy by Design:

1. *"Proactive not Reactive; Preventative not Remedial* (It anticipates and prevents privacy invasive events before they happen.)
2. *Privacy as the Default* (No action is required on the part of the individual to protect their privacy – it is built into the system, by default.)
3. *Privacy Embedded into Design* (Embedded into the design and architecture of IT systems and business)
4. *Full Functionality – Positive-Sum, not Zero-Sum* (no unnecessary trade-offs are made...it is possible to have both privacy and security)
5. *End-to-End Lifecycle Protection* (at the end of the process, all data are securely destroyed, in a timely fashion)
6. *Visibility and Transparency* (Its component parts and operations remain visible and transparent, to users and providers alike.)
7. *Respect for User Privacy* (Keep the interests of the individual uppermost)."¹⁴¹

¹³⁹Article 29 WP, Opinion 168, The Future of Privacy -Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf in Art. 29 WP Opinion 183

¹⁴⁰<http://privacybydesign.ca/about/>, accessed on November 2011

¹⁴¹Cavoukian Ann, Polonetsky Jules, Wolf Christopher,, *Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation*, 2009, available at <http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=912> or <http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf>

In the case of Smart Grids it is necessary to work with the privacy measures from the beginning, even though in some countries (for example Italy or California) the smart meters have already been installed. The aim should be to process minimum personal data possible. Article 29 Working Party wish that if implemented, Privacy by Design would ensure that meter readings are only transmitted as frequently as necessary for their operation or for the service that customer agreed to.¹⁴² The question is how to best proceed with implementation of Privacy by Design. There should be legislative requirements for such principle (as in the case of DRMS). Also data controllers and processors should put in place appropriate measures for better protection of personal data. DSOs or energy suppliers could build up their own technical infrastructure for Privacy by Design. Even though this might be costly in the beginning, it would still be more efficient than to do it later. If privacy friendly system is established, data controllers should then carefully decide what data need to be personalized for their purposes. Utilities nowadays argue that they need personal data for billing purposes. Experts Danezis and Rial came lately with results of their research where they claim that "unlike what the common wisdom dictates, none of their solutions require privacy-invasion for the purpose of billing."¹⁴³

Ideally, Privacy by Design would combine privacy enhancing technologies, privacy by default and encryption.¹⁴⁴ It should cover the whole information system of the Grid, from meter to back-office, to support, to the financial department.¹⁴⁵ Privacy by Design should be designed in a way that the lowest possible data volumes are processed and transmitted.

¹⁴²Art 29 WP, Opinion 183

¹⁴³Danezis George, Rial Alfredo, *Privacy Preserving Metering for Smart Grids*, 2010, available at <http://research.microsoft.com/en-us/um/people/gdane/pfsm.pdf.pdf>, accessed on November 2011 – They argue "Naively, there seems to be a balance to be struck between the intrusion necessary for billing, and the claimed social benefits of smart-grids. We show this intuition to be false, and present practical privacy-friendly metering systems that do not necessarily leak any information to third parties while providing unforgeable bills based on complex dynamic tariff policies"

¹⁴⁴Privacy enhancing technologies (PETs), could be described as a system of ICT measures protecting privacy - other definitions can be found in Burkert, H. "Privacy Enhancing Technologies: Typology, Critique, Vision" In Agre, Philip, and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, Mass.: MIT Press, 1997.

¹⁴⁵Expert Group 2, draft report from 6.6.2011

As one can see, there are ways how to protect personal data within Smart Grids, Privacy by Design is only one of those solutions. Some of these issues were tackled above, some of the remaining can be again inspired by Ann Cavoukian. In her concept "Smart Privacy for the Smart Grid", she presents the following points (some were mentioned in this thesis before):

- utilities should collect only the minimum amount of personal data necessary for providing the service;
- utilities should be transparent about the personal data collection towards their customer's;
- privacy should be build in systems prior their use;
- when the personal information is not needed it should be securely disposed;
- consumers should be able to tailor their personal information options;
- utilities should be proactive when getting consumer's consent for personal data disclosure to third parties;
- individuals would have access to their data files and would be able to correct mistakes;
- privacy by default together with security protocols should help to protect personal data against security breaches and data leakage;
- improve consumers confidence and environment awareness by tackling all the problems which would lead towards increased trust in Smart Grids¹⁴⁶

Combination of these key issues might enhance privacy and data protection in the intelligent networks. If we elaborate on some of those points further, it can be agreed that all companies that have some ties to Smart Grids/smart meters should have some form of privacy training on a regular basis (employees who work with this matter should be educated in the privacy and data protection field). Not only utilities vendors but also public should be aware of the privacy and data protection implications. If we look at the

¹⁴⁶Cavoukian Ann, Polonetsky Jules, Wolf Christopher, *Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation*, 2009

example of some social networks, we are witnessing people who do not care about their privacy settings. Some of them do not care, others might not be aware of all the options they have. At least for those who are concerned with these issues, there should be guidance from the utilities on how to protect privacy.

To sum up, Privacy by Design is one of the possible solutions to the data protection problems of Smart Grids. If this concept will be used together with other suggested measures, for example Smart Privacy for the Smart Grid, it could help with some of the privacy implications of the intelligent networks.

4.2 Analysis of the recommendations of the Expert Group 2 (draft June 2011 report)

The recommendations of the Task Force Expert Group 2 from the draft June 2011 report are presented in detail below. This document can be so far considered as the most elaborated and detailed recommendation for the Smart Grids in the EU. It is, however, necessary to evaluate the applicability of its recommendations (analysis can be found under each recommendation):

1) ... *"It is recommended to address the Member States to review their regulatory frameworks in order to be able to enforce the use of common standards across the European Union."*¹⁴⁷

The review of the regulatory frameworks could be a lengthy and complicated process. The Member States should have a clear deadline for the revision (to avoid delays). More effective solution could be to prepare one EU document with applicability across the EU. MS's would have time to address their comments to the text within specific time-frame.

2) *"...it is recommended to confirm that in accordance with opinion 183 of the Article 29 Data Protection Working Party most data from Smart Grids can be considered personal data..."*¹⁴⁸

¹⁴⁷Task Force Smart Grids, Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection- final draft*, issued on 6.6.2011

¹⁴⁸Expert Group 2, draft report from 6.6.2011

The above mentioned recommendation is supported by this thesis (presented in chapter 3). As shown in the legal analysis (chapter 3.1), since Smart Grids data could reveal the most intimate details of private lives as well as the most sensitive information from the businesses, a proper legal framework with safeguards for customers needs to be established.

3) *"The implementation of Smart Grids potentially connects location information to specific data that holds information on the use of electrical energy, and in the future possibly more....It is recommended that adequate measures are deployed to protect the contents and nature of this data in order to safeguard the privacy of the consumer."*¹⁴⁹

A variety of measures, such as data anonymisation or Smart Grids operation based on non-identifiable data were suggested to protect consumers privacy. These solutions might not be sufficient. According to some experts even anonymised data may reveal an individual when combined with other types of anonymous data.¹⁵⁰ So far, there is no direct evidence about the possibilities of de-anonymisation in the Smart Grids. Expert Group 2 is however suggesting that the threat of de-anonymisation is serious.¹⁵¹ It is thus important that more research is done in the field of anonymisation. The European Commission should support these projects financially.

4) *"Privacy by Design and by Default should be strongly encouraged..."*¹⁵²

Currently, Privacy by Design and by Default seem to be one of the main solutions for Smart Grids data protection. As with the above mentioned anonymisation, the European Commission should financially support research, development and pilot projects with the aim of integrating Privacy by Design to the Smart Grids functionalities from the very beginning. Although none of the technologies is perfect, it is so far the best possible option. One should bear in mind that Privacy by Design should have proper support in the legal framework.

5) *"Performing (a form of) Privacy Impact Assessments on Smart Grid developments should be encouraged..."*¹⁵³

Privacy Impact Assessments (PIAs) can help to evaluate whether Smart Grids components and policies meet legal privacy requirements. PIA also examines the public

¹⁴⁹Expert Group 2, draft report from 6.6.2011

¹⁵⁰National Institute of Standards and Technology, (NISTIR 7628). The Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, August 2010, page 25 or Efthymiou Costas, Kalogridis Georgios, *Smart Grid Privacy via anonymization of Smart Metering Data*, 2010 or Ohm P. *Broken promises of privacy: responding to the surprising failure of anonymization*, Legal Studies Research Paper No. 09-12, University of Colorado Law, 2009.

¹⁵¹Expert Group 2, draft report from 6.6.2011

¹⁵²Ibid.

¹⁵³ Ibid.

opinions; this could anticipate reactions to the planned massive roll-out of smart meters in the EU. Since the privacy implications would be considered from the beginning, costs for the technological solutions would be lowered. States as well as private companies could save time and money if performing PIA before widespread deployment of Smart Grids. The European Commission should support PIAs financially from its framework programmes (such as The Seventh Framework Programme or Intelligent Energy Programme) since such assessments might be quite costly.

6) *"Given the variety of data storage purposes within smart metering, a single data retention period cannot be concluded."*¹⁵⁴...

Since the Member States criminal and civil procedures might differ, the data retention must be left up to the countries themselves (in issues such as taxation). On the other hand, Article 29 Data Protection Working Party states that 13 months period of data retention could be an appropriate period for offering year on year comparisons for energy efficiency purposes (other services should have shorter period of retention).¹⁵⁵ Customers across the EU should be informed about the maximum data retention period and they should be able to challenge unfair data storage at independent body (ombudsman or European Data Protection Supervisor).

7) *"EG2 recommends to perform an analysis in order to determine to which extent utilities need to retain personal data (i.e. neither non-aggregated nor anonymised) to be able to maintain the electrical grid and perform billing."*¹⁵⁶

It is above the level of expertise of this thesis to come with my own proposals to this issue. Expert Group 2 suggests encryption as a mechanism for utilities data retention.¹⁵⁷

8) *"The following principles should apply for the purpose of data retention: (a) data minimisation – i.e. the scope and length of both (i) data collection and (ii) data retention shall in any case not exceed absolute minimum; (b) transparency – i.e. who, when and in what circumstances collects, processes and retains personal data, and what data and where are stored; (c) empowerment of the consumer – i.e. safeguarding consumer's rights (including information) and their participation."*¹⁵⁸

Data controllers and processor should stick to these principles. However, there is still a lot to be done. It would be necessary to prepare guidance documents for the data retention purposes in Smart Grids/meters, preferably by the EU authorities with a margin of appreciation for the states. One also needs to consider the issue of third parties. What

¹⁵⁴ Expert Group 2, draft report from 6.6.2011

¹⁵⁵ Art 29 WP, Opinion 183

¹⁵⁶ Expert Group 2, draft report from 6.6.2011

¹⁵⁷ Ibid.

¹⁵⁸ Ibid.

if the third party comes from a state outside of EU where there is no adequate level of protection?¹⁵⁹ In such a case, it would be advisable that no data relating to individuals should be accessible to those parties. "Special care has to be taken if approaches like cloud computing are used, where data handling is often not transparent."¹⁶⁰

9) *"The use of privacy certification schemes should be encouraged...It should be left to the regulatory bodies to determine which certification scheme and structure should be used."*¹⁶¹

Privacy certificates could ensure data subjects that Smart Grid actors are obeying the rules of current data protection framework. Such certification already exists for other sectors. The European legislators should come with a list of criteria that needs to be finalised early enough, not to delay intelligent networks deployment.

10) ... *"In order to be able to adequately protect consumer rights and enable the effective use of Smart Grids DPAs need to be involved in the process, but also need to be able to apply a consistent set of responsibilities, definitions and principles"*¹⁶²...

DPAs should coordinate their activities across the EU. Smart Grids will be more interconnected in the future; harmonization of the data protection in this area is thus advisable. As recommended, DPAs should be more involved during the process of preparing relevant legislation and the actual implementation and enforcement of these rules.

11) *"Non-compliance with privacy limitation criteria might have an adverse effect on Smart Grids deployment in a given electricity market. Both enactment of a regulatory framework and a practice that respect these limitation criteria will minimise such a risk."*¹⁶³

The chapter 3.10 evaluated whether the existing Smart Grid framework would satisfy the privacy criteria required by the ECHR, CFR and national legislation. The current situation is not very clear and differ state from state. As could be seen in the Dutch example, the proposed bill was found incompatible with the Article 8 of ECHR which resulted in changing of the controversial legislation. This issue contributed to the scepticism of consumers and could have threatened the smart meters roll-out in the Netherlands. Such situation should be prevented. The freedom of choice for customers should be an important criterion when drafting the legal framework and enforcing the

¹⁵⁹Data Protection Directive, Article 25 deals with transfers of data to third countries.

¹⁶⁰Expert Group 2, draft report from 6.6.2011

¹⁶¹Ibid.

¹⁶²Ibid.

¹⁶³Ibid.

legislation. Also campaigns to raise people's awareness about Smart Grids could be the first step towards successful implementation of smart metering in Europe.

*12) "It is recommended that the Commission provides evidence that allows to assess whether smart metering's interference with privacy is permissible, i.e. whether it is in accordance with the principles of legality, legitimacy, necessity and proportionality. In addition, it is recommended that specific measures are taken to ensure the adequate protection of personal data in smart metering. Data logging procedures for updates and broadcast to meters can aid in achieving this goal, and should be considered."*¹⁶⁴

As shown in the part on Privacy in the Smart Grids, it is necessary to make privacy impact assessments where states would be able to justify smart metering interference with privacy. Evaluation of the above mentioned criteria should be done on the state and European level. If it is found unsatisfactory (insufficient), an EU-wide regulation that would control privacy implications of Smart Grids should

*12) "It is recommended that the Commission provides evidence that allows to assess whether smart metering's interference with privacy is permissible, i.e. whether it is in accordance with the principles of legality, legitimacy, necessity and proportionality. In addition, it is recommended that specific measures are taken to ensure the adequate protection of personal data in smart metering. Data logging procedures for updates and broadcast to meters can aid in achieving this goal, and should be considered."*¹⁶⁵

As shown in the part on Privacy in the Smart Grids, it is necessary to make privacy impact assessments where states would be able to justify smart metering interference with privacy. Evaluation of the above mentioned criteria should be done on the state and European level. If it is found unsatisfactory (insufficient), an EU-wide regulation that would control privacy implications of Smart Grids should be considered.

Having evaluated the above mentioned draft report, it can be said that most of its recommendations are sound and reasonable. Overall, the report meets all requirements and does not need to be subject of any heavy criticisms.

¹⁶⁴Expert Group 2, draft report from 6.6.2011

¹⁶⁵ Ibid.

5. Conclusion

In this thesis, the current legal privacy and data protection framework regarding Smart Grids/smart metering was considered. It was concluded that since personal data are collected, processed and transferred in smart meters, the European data protection framework applies to Smart Grids.

Evaluation of the current legal framework, however, showed that some of the provisions of the directives or other legal documents does not provide sufficient protection for the data subjects. Since the reality of Smart Grids/smart metering could influence almost every aspect of our lives, it is necessary to provide safeguards that would persuade people that their fundamental right to privacy and data protection would not be harmed. This could be done through an improvement of current legislation on the EU level. It is recommended to draft an EU wide regulation for Smart Grids which would guarantee equal implementation of the privacy criteria among the EU Member States. Countries could have a margin of manoeuvre for specific issues that cannot be harmonized on the EU level (such as different periods for data retention).

Important factor is speed and effectiveness of the suggested legislative changes. In some countries, the smart meters roll-out has already started. It is advisable the countries would harmonize their approach with the Data Protection Authorities as well as data controllers. Privacy Impact Assessments should be speed up and their results should be consulted with all the relevant actors in the Smart Grids environment.

Legislation should be complimented with Privacy by Design and other possible measures (such as privacy certificates of privacy friendly companies, technical solutions encompassing Privacy by Default etc.) from the beginning. The intrusive marketing on behalf of third parties must be prevented since this is one of the main concerns people have with respect of smart metering.

Public awareness and education should be, inter alia, an important part of the strategy for smart metering roll out in the EU. Only informed consumers could really contribute to the success of energy efficiency measures that European Union plans. All in all, a complex system of measures should be used in order to convince public that their privacy and data protection within Smart Grids would be ensured.

6. References

European Union:

1. Charter of Fundamental Rights of the European Union 2000/C 364/01. s.l. :Official Journal of the European Communities, 2000.
2. 2007/C 306/01 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. 2007.
3. C 11 5/47 The Treaty on the Functioning of the European Union. 2008.
4. C 115/13 Treaty on the European Union. 2008.

EC Directives:

5. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. 24 October 1995.
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. 12 July 2002.
7. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. 2006.
8. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services. 25 November 2009.
9. Directive 2009/72/EC of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. 2009.
10. Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments. 2004.

Council of Europe:

11. European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 (ECHR).

Article 29 Data Protection Working Party:

12. **Article 29 Data Protection Working Party.** *Opinion 12/2011 on smart metering* (adopted on 4 April 2011).
13. **Working Party 29.** *Opinion 15/2011 on the definition of consent* (adopted on 13 July 2011).
14. **Working Party 29.** *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. (adopted on 1 December 2009).*
15. **Working Party 29.** *Opinion 1/2010 on the concepts of “controller” and “processor”* (adopted on 16 February 2010).

Other documents:

16. Task Force Smart Grids, Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection- final draft*, issued on 6.6.2011
17. Task Force Smart Grids, Expert Group 2, *Regulatory Recommendations for data safety, data handling and data protection*, report issued 16.2.2011
18. European Commission, *Smart Grids: from innovation to deployment; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, Brussels, 12.4.2011
19. European Commission, Directorate-General Energy, Directorate B- Security of Supply and Energy Markets, *Meeting minutes from the 9th meeting of the Steering Committee of the Task Force for Smart Grids*, 15.6.2011
20. European Data Protection Supervisor, Letter from Assistant Supervisor to Mr Günther Oettinger, Commissioner for Energy - *Proposal for a Directive of the*

European Parliament and of the Council on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC, 27.10.2011

21. Joint Research Centre, *Smart Grid projects in Europe: lessons learned and current developments*, 2011
22. Germany Federal Constitutional Court - Press office, *Data retention unconstitutional in its present form*, Press release no. 11/2010 of 2 March 2010
23. Department of Energy and Climate Change, *Smart Metering Implementation Programme – A call for evidence on data access and privacy*, August 2011
24. National Institute of Standards and Technology, (NISTIR 7628). The Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, August 2010

Articles:

25. Gershuny, Deana, *International smart meter roll-out sparks privacy concerns*, Privacy Laws&Business International Newsletter, December 2010
26. Smart meters: Controlling your energy bill? (available at <http://www.euractiv.com/en/energy-efficiency/smart-meters-controlling-your-energy-bill-links dossier-257199>), accessed on July 2011
27. Keith Nuthall, *EU smart grids privacy legislation under discussion*, Utility Week (1. July 2011), http://www.utilityweek.co.uk/news/news_story.asp?id=195596&title=EU+smart+grids+privacy+legislation+under+discussion, accessed on July 2011

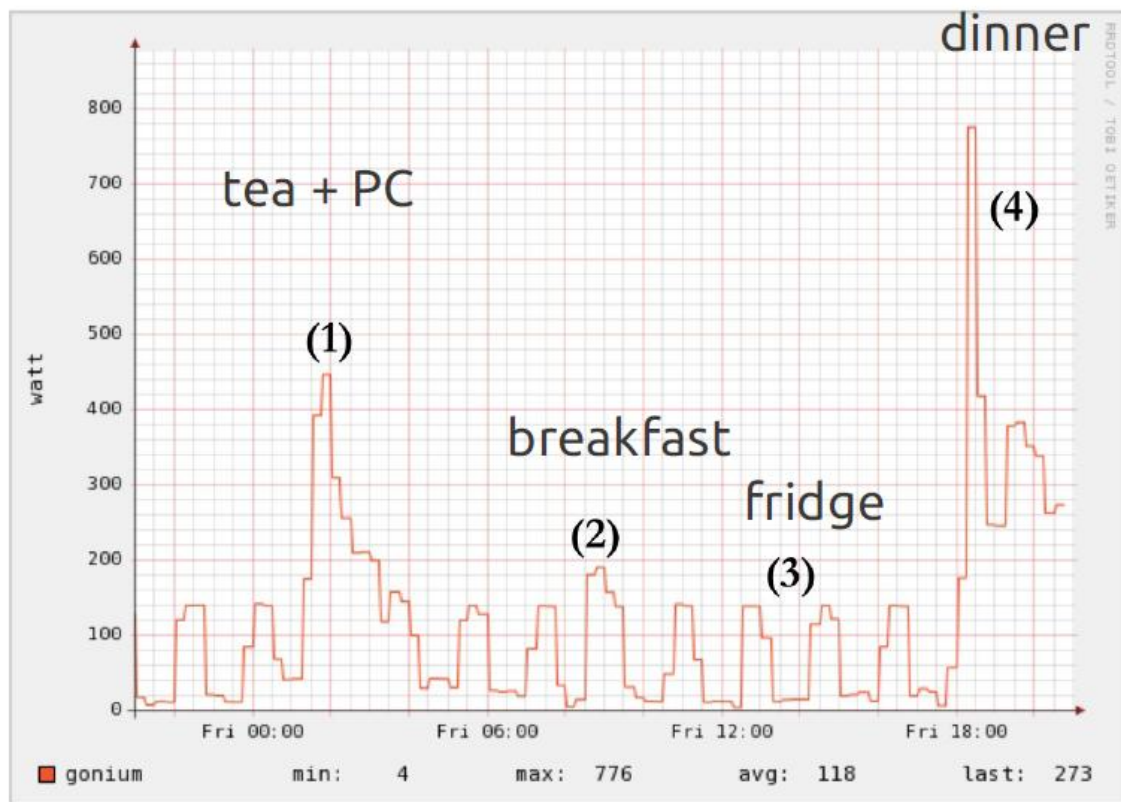
Literature:

28. Balough, Cheryl, Dancey, *Privacy Implications of Smart Meters*, Chicago-Kent Law Review, 2011
29. Burkert, Herbert, *Privacy Enhancing Technologies: Typology, Critique, Vision* in Agre, Philip, and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, Mass.: MIT Press, 1997.
30. Bygrave, Lee. Andrew, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague/London/New York: Kluwer Law International, 2002.
31. Bygrave, Lee. Andrew, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, 1998, volume 6, pp. 247-284

32. Bygrave, Lee. Andrew, *Privacy and Data Protection in an International Perspective*, Stockholm Institute for Scandinavian Law, 2010.
33. Cavoukian Ann, Polonetsky Jules, Wolf Christopher., *Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation*, *Identity in the Information Society* 3 (2):275-294 ,2010
34. Danezis George, Rial Alfredo, *Privacy Preserving Metering for Smart Grids*, 2010
35. Efthymiou Costas, Kalogridis Georgios, *Smart Grid Privacy via anonymization of Smart Metering Data*, IEEE International Conference on Smart Grids Communications, 2010
36. Knyrim, Rainer, Trieb, Gerald., *Smart metering under EU Data Protection Law*, *International Data Privacy Law*, 2011, Vol. 1, No. 2
37. Ohm, Paul, *Broken promises of privacy: responding to the surprising failure of anonymization*, Legal Studies Research Paper No. 09-12, University of Colorado Law, 2009.
38. Solove, Daniel, *Understanding Privacy*, Harvard University Press, Cambridge, Massachusetts 2008
39. Warren, Samuel, D. and Brandeis, Luis, D. , *The Right to Privacy*, *Harvard Law Review*, 1890, p. Vol.4 No.5.
40. Westin, Alan, F., *Privacy and Freedom*, Atheneum, New York 1970

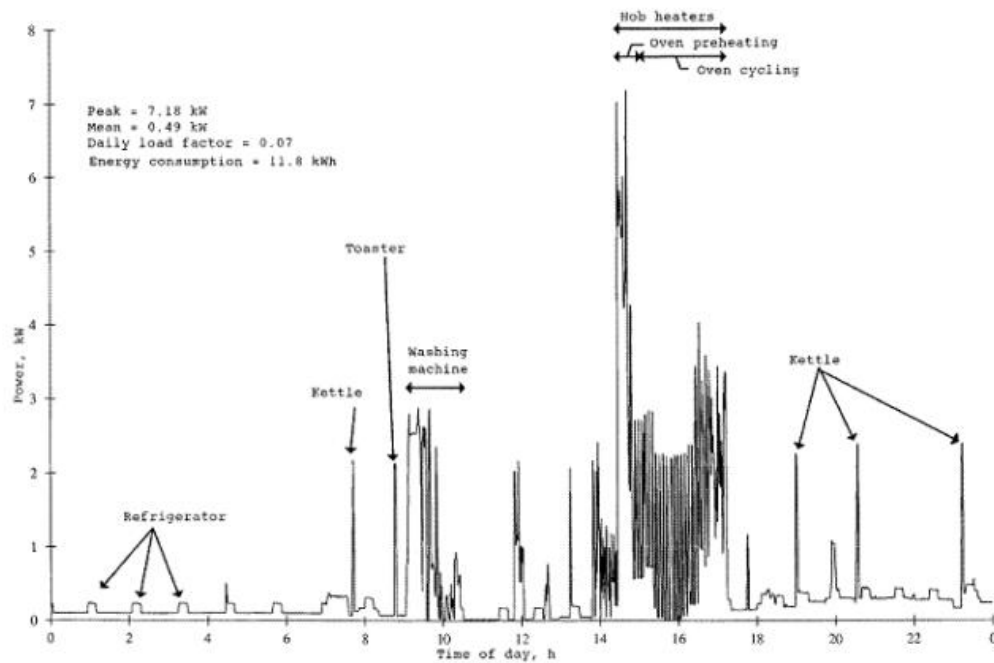
7. Annexes

Examples of smart meter readings:



<https://www.mysmartgrid.de>

Source: www.mysmartgrid.de



Source: National Institute of Standards and Technology, (NISTIR 7628). The Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, August 2010